Google Chrome tiene una vulnerabilidad grave, por lo que es necesario que actualices el navegador a la última versión inmediatamente.

Clement Lecigne, investigador de seguridad del grupo de análisis de amenazas de Google, descubrió y reportó una vulnerabilidad de alta gravedad en Chrome a finales del mes pasado, que podría permitir a los atacantes remotos ejecutar código arbitrario y tomar el control total de las computadoras.

La vulnerabilidad CVE-2019-5786 afecta el software de navegación web para todos los principales sistemas operativos, como Windows, MacOS y Linux.

Aún no se han revelado detalles técnicos sobre la vulnerabilidad, pero el equipo de seguridad de Chrome dice que el problema se debe al uso del componente FileReader del navegador, que conduce a ataques de ejecución remota de código.

Google advirtió que esta vulnerabilidad de RCE de día cero está siendo explotada de forma activa por los atacantes.

> *«El acceso a los detalles de los errores y los enlaces puede mantenerse restringido hasta que la mayoría de los usuarios se actualicen con una solución. También mantendremos restricciones si el error existe en una biblioteca de terceros de la que otros proyectos dependen de forma similar, pero aún no se ha solucionado»*, dice el equipo de seguridad de Chrome.

FileReader es una API estándar que fue diseñada para permitir que las aplicaciones web lean de forma asíncrona el contenido de los archivos almacenados en la computadora del usuario, utilizando los objetos «Archivo» o «Blob» para especificar el archivo o datos para leer.

La vulnerabilidad libre después de uso es una clase de error de corrupción de memoria que permite la corrupción o modificación de los datos en la memoria, lo que permite a un usuarios sin privilegios escalar privilegios en un sistema o software afectado.

Además, permite a los atacantes sin privilegios, obtenerlos en el navegador web Chrome, permitiéndoles escapar de las protecciones de la zona de pruebas y ejecutar código arbitrario en el sistema seleccionado.

El atacante al explotar la vulnerabilidad, solo debe engañar a las víctimas para que abran o redirijan a una página web especialmente diseñada sin necesidad de interacción adicional.

El parche para dicha vulnerabilidad ya se extendió a sus usuarios en una actualización de Chrome estable, la 72.0.3626.121 para los sistemas operativos Windows, Mac y Linux, que los usuarios pueden haber recibido o recibirán pronto.